

European Patent Application

„Message Authentication“

Sony International (Europe) GmbH

S99P5143EP00/PAE99-080TRDE

5 P22953

### Abstract

10 For the authentication of messages communicated in a distributed system from an  
originator to a destination a keyed-hashing technique is used according to which data to  
be authenticated is concatenated with a private (secret) key and then processed to the  
cryptographic hash function. The data are transmitted together with the digest of the  
hash function from the originator to the destination. The data comprises temporal  
15 validity information representing the temporal validity of the data. For example the  
setup key of a communication is therefore only valid within a given time interval that is  
dynamically defined by the communication originator. After the time interval is  
exceeded the setup key is invalid and cannot be reused again.

20 (Figure 1)